



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/540,219	01/17/2006	Jean-Bernard Fischer	0579-1097	5286
466 7590 03/22/2010 YOUNG & THOMPSON 209 Madison Street Suite 500 Alexandria, VA 22314			EXAMINER VAUGHAN, MICHAEL R	
			ART UNIT 2431	PAPER NUMBER
			NOTIFICATION DATE 03/22/2010	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketingDept@young-thompson.com

Office Action Summary

Application No.

10/540,219

Applicant(s)

FISCHER ET AL.

Examiner

MICHAEL R. VAUGHAN

Art Unit

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 February 2010.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9, 11-21, 23-30, 32, 33 and 35-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9, 11-21, 23-30, 32, 33, 35-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **2/4/10** has been entered.

Claims 1-9, 11-21, 23-30, 32, 33, 35-40 are pending. Claims 1, 17, and 26 have been amended.

Response to Amendment

Claim Objections

The current claim amendment is sufficient in overcoming the previous claim objection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-9, 11-21, 23-30, 32, 33, 35-40 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The current claim amendment has required the at least one second instruction to control the calculation **mode** (emphasis added). The original specification provides support for a plurality of instructions including one which administers the actual calculation of the second signature. However, there is no support for a calculation mode of a signature. A calculation mode carries with it the inherent choice between more than type of signature calculation algorithms. The original disclosure is absent such a teaching. Applicant has cited instructions A2, A12, B7, C7, C8, and D11 as support for this new limitation again. After closer inspection however, these instructions do not appear to control the calculation mode. They appear to assist in the actual calculations of the second signature but not the mode of said calculations.

Response to Arguments

Applicant's arguments filed 2/4/10 have been fully considered but they are not persuasive. The following interpretation of the prior art is solely based on the current set of claims and arguments submitted by the Applicant. It is not the only possible

interpretation of the prior art and may be altered when/if the claims and/or arguments change.

Applicant alleges that Naccache fails to teach a second instruction for controlling the calculation mode of the second signature. First of all, as pointed out above, the original disclosure is silent in providing support for a second instruction for controlling the calculation mode of the second signature. Nevertheless, in case support is found, both the claims as amended and the arguments have been fully considered. The arguments assert repeatedly that Naccache fails to teach a second instruction for controlling the calculation of the signature. The point here is, that the arguments seem to take the position that the second instruction is for controlling the calculation of the signature, not the calculation mode of the signature. The difference while subtle has profound implications. For one, the application does not seem to support the idea of an instruction determining the mode of calculation but rather just calculates the signature as intended. There does not seem to be dynamic determination. Secondly, with the respect to the prior art, Naccache appears to teach an instruction which does control the calculation of the second signature (see. Fig. 3, element 40). This step produces a hash (signature) of the instruction by instantiating the function F.

Applicant has noted that the claims differ from the prior art because the claimed invention has three distinct monitoring instructions. From page 20 of the response, they are (1) for initializing the calculation of a signature, (2) controlling the calculation of the signature, and (3) comparing the calculated signature with another. All three can be found in Figure 3 of Naccache: (1) is equivalent to transitioning from step 32 to the

initialization in step 34, (2) corresponds to step 40 which calculates a signature hash, and (3) is found at comparison step 50.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 8, 9, 11-21, 23-28, 32, 33, and 35-40 are rejected under 35 U.S.C. 102(e) as being anticipated by USP 7,168,065 to Naccache et al, hereinafter Naccache.

As per claim 1, Naccache teaches a method of making secure the execution of a computer program (EXE) including a set of at least one instruction, which method is characterized in that it includes:

- a first step (E30), prior to the execution of the computer program, of calculating and storing a first signature (SIG1) representative of the intended execution of the set of instructions (col. 4, lines 25-29),
- a second step (E50), during the execution of the set of instructions, of calculating and storing a second signature (SIG2) representative of the execution of the set of

instructions (col. 4, lines 35-36), and

- a step (E60) of detecting an anomaly in the execution of the set of instructions on the basis of the first signature (SIG1) and the second signature (SIG2) (col. 4, lines 38-39), wherein said set of instructions comprising at least one first instruction for initializing the calculation of the second signature (col. 9, lines 25-30 and Fig. 3, element 34), at least one second instruction for controlling the calculation mode of the second signature (Fig. 3, element 40, and col. 9, lines 34-40), and a third instruction, different than the at least one second instruction, for comparing the second signature obtained according to the at least one second instruction with the first signature (col. 9, lines 51-55 and Fig. 3, element 50).

As per claim 26, Naccache teaches a device for making secure the execution of a computer program including a set of instructions comprising at least one instruction, which device is characterized in that it includes (see abstract):

- a first register (REG1) (col. 4, line 8) for storing a first signature (SIG1) representative of the intended execution of the set of instructions (col. 4, lines 25-29),
- means (22) for calculating and storing in a second storage register (REG2) (col. 6, line 18) during the execution of the set of instructions a second signature (SIG2) representative of the execution of the set of instructions (col. 4, lines 35-36), and
- means (24) for detecting an anomaly in the execution of the set of instructions on the basis of the first signature (SIG1) and the second signature (SIG2) (col. 4, lines 35-36),

said set of instructions comprising at least one first instruction for initializing the calculation of the second signature (col. 9, lines 25-30 and Fig. 3, element 34), at least one second instruction for controlling the calculation mode of the second signature (Fig. 3, element 40, and col. 9, lines 34-40), and a third instruction, different than the at least one second instruction, for comparing the second signature obtained according to the at least one second instruction with the first signature (col. 9, lines 51-55 and Fig. 3, element 50).

As per claim 2, Naccache teaches that the first calculation and storage step (E30) is executed during the generation [preparation] of the instructions (AI, AI3) of the computer program (col. 4, line 25).

As per claims 3 and 27, Naccache teaches that the second signature (SIG2) stored during the second calculation and storage step (E50) is retained in memory during the execution of at least one second instruction following the set of instructions (col. 5, lines 4-6 and 64-68). Naccache teaches using one the preceding values in memory to calculate the next value, so therefore it must remain in memory.

As per claims 4 and 28, Naccache teaches the first signature (SIG1) is obtained from the number of instructions in the set of instructions [accounts for each number of the instructions] (col. 9, lines 23-27),

- the second signature (SIG2) is obtained from the number of instructions from the set of instructions that have been executed [numerical value of executed instructions](col. 9,

lines 31-35), and in that

the detection step (E60) detects an execution anomaly when the first signature (SIG1) and the second signature (SIG2) are different after the execution of the set of instructions [compare VHN to Vref] (col. 9, lines 60-64).

As per claims 8 and 32, Naccache teaches the first signature (SIG1) is obtained from the code of a critical instruction of the set of instructions (col. 4, lines 25-29),

- the second signature is obtained from the code of the critical instruction, that code being stored at the same time as or after the execution of the critical instruction [jump] (col. 14, lines 32-35), and in that

- the detection step (E60) detects an execution anomaly when the first signature (SIG1) and the second signature (SIG2) are different after the execution of the set of instructions (col. 10, lines 14-19).

As per claims 9 and 33, Naccache teaches the first signature (SIG1) is obtained from the address of a critical instruction (col. 5, line 51) of the set of instructions, the address being obtained during or after the generation of the executable code of the set of instructions (col. 4, lines 25-29),

- the second signature (SIG2) is obtained from the address of the critical instruction, that address being stored (E30) at the same time as or after the execution (E30) of the critical instruction (col. 14, lines 32-38), and

- the detection step (E60) detects an execution anomaly when the first signature (SIG1) and the second signature (SIG2) are different after the execution of the set of instructions (col. 10, lines 14-19).

As per claims 11 and 35, Naccache teaches the first signature (SIG1) and the second signature (SIG2) are error detector codes (CRC1, CRC2) calculated from the code or from an address of an instruction of the set of instructions (col. 5, lines 53-58), and in that the detection step (E60) detects an execution anomaly when the first signature (SIG1) and the second signature (SIG2) are different after the execution of the set of instructions (col. 10, lines 14-19).

As per claims 12 and 36, Naccache teaches that the error detector codes are cyclic redundancy check codes (col. 5, lines 53-58).

As per claims 13 and 37, Naccache teaches that the error detector codes are obtained by the logical combination (XOR) of the code or an address of at least one instruction of the set of instructions (col. 5, lines 53-58). Naccache teaches the use of CRC which perform logical combination (XOR included) in order to carry out the operation. Examiner is not giving XOR patentable weight here as the syntax implies XOR as an example of logical combination.

As per claims 14 and 38, Naccache teaches the first signature (SIG1) and the second signature (SIG2) are respectively obtained during the generation and the execution of the instructions from at least two elements chosen from:
the number of instructions in the set of instructions,
the **code** of at least one instruction of the set of instructions (col. 5, lines 45-51),
the **address** of at least one instruction of the set of instructions (col. 5, lines 45-51), and
an error detector code calculated from the code or an address of at least one critical instruction of the set of instructions, the address being obtained during or after the

generation of the executable code of the set of instructions (col. 5, lines 53-59), and in that the detection step (E60) detects an execution anomaly when the first signature (SIG1) and the second signature (SIG2) are different after the execution of the set of instructions (col. 10, lines 14-19). Naccache teaches using the code and address as hash inputs thus two criteria from the list are chosen.

As per claims 15 and 39, Naccache teaches that it includes a step (E70) of destroying at least a portion of the system on which the computer program is executed, this step of destroying being made when an execution anomaly is detected in the detection step (col. 4, line 45).

As per claim 16, Naccache teaches in that the first signature (SIG1) is generated automatically [already generated before execution of program] (col. 4, line 25-30).

As per claim 17, Naccache teaches a device for processing a computer program including a set of at least one instruction, characterized in that it includes means (12) for calculating and storing a first signature (SIG1), the first signature (SIG1) stored in a memory and the first signature is representative of the intended execution of the set of instructions prior to the execution thereof (col. 4, lines 25-30), said set of instructions comprising at least one first instruction for initializing the calculation of the second signature (col. 9, lines 25-30 and Fig. 3, element 34), at least one second instruction for controlling the calculation mode of the second signature (Fig. 3, element 40, and col. 9, lines 34-40), and a third instruction, different than the at least one second instruction, for

comparing the second signature obtained according to the at least one second instruction with the first signature (col. 9, lines 51-55 and Fig. 3, element 50).

As per claim 18, Naccache teaches the first signature (SIG1) [Vref] are adapted to calculate and store information obtained from the number of instructions of the set of instructions (col. 9, line 65 - col. 10, line 5).

As per claim 19, Naccache teaches the means (12) for calculating and storing the first signature (SIG1) are adapted to obtain and store information obtained from the code of a critical instruction [jump] of the set of instructions (col. 14, lines 33-35).

As per claim 20, Naccache teaches means for generating executable code from the computer program (col. 8, lines 35-36).

As per claim 21, Naccache teaches the means for calculating and storing the first signature (SIG1) are adapted to obtain and store information obtained from the address of a critical instruction (col. 5, line 51), the information being obtained of the set of instructions by the means (14) for generating executable code (col. 8, lines 35-40).

As per claim 23, Naccache teaches that the means (12) for calculating and storing the first signature (SIG1) are adapted to calculate and store information obtained from an error detector code (CRC1) calculated from the code or an address of at least one instruction of the set of instructions (col. 5, lines 53-58).

As per claim 24, Naccache teaches that the error detector code (CRC1) is a cyclic redundancy check code (col. 5, line 57).

As per claim 25, Naccache teaches that the error detector code is obtained by a logical combination (XOR) of the code or an address of at least one instruction of the set of instructions (col. 5, lines 53-58). Naccache teaches the use of CRC which perform logical combination (XOR included) in order to carry out the operation. Examiner is not giving XOR patentable weight here as the syntax implies XOR as an example of logical combination.

As per claim 40, Naccache teaches a microcircuit card [smart card] characterized in that it includes a securing device according to claim 26 (col. 6, lines 27-35).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5-7, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache.

As per claims 5 and 29, Naccache teaches the first signature (SIG1) is obtained from the number of instructions in the set of instructions [accounts for each number of the instructions] (col. 9, lines 23-27). The calculation performed in these claims is an obvious mathematical variation to those taught by Naccache and in claim 4. Claim 4

calculates a running hash value by each of executed instructions and ultimately compares the final result to the reference hash value. This ensures that each instruction is proper and that the instructions in the set are executed in the correct order. One of ordinary skill in the art could have simply run the hash on the unexecuted instructions and subtracted that value to the reference hash to achieve the same desired result. This provides the same assurance that each proper instruction was executed in the correct order. Once all of the instructions are executed, the value should be zero if they all matched the reference hash value. This is simply an operational design choice. The claim would have obvious because one of ordinary skill in the art can substitute equivalent known methods which yield predictable results.

As per claims 6 and 30, Naccache teaches that an interrupt of the computer program is triggered when the value of the second signature (SIG2) is below a predetermined threshold (col. 4, lines 40-47).

As per claims 7, Naccache teaches that the first signature (SIG1) and the second signature (SIG2) are retained in memory (col. 1, line 47) during the execution of the program in the same register (REG1) (col. 9, lines 13-17).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am

- 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431